Section 2

INTRUSION DETECTION AND ASSESSMENT

Contents

References 2-1
General Information 2-1
Common Deficiencies/Potential Concerns..2-3
Planning Activities 2-4
Performance Tests...2-5
Data-Collection Activities...2-5

References

DOE Order 5632.1C
DOE Manual 5632.1C-1

General Information

DOE Order 5632.1C stipulates that unauthorized intrusion be detected by the use of alarm systems, random patrols, or visual surveillance. The standard is applicable to property protection areas, limited areas (LAs), exclusion areas, secure communication centers, PAs, MAAs, and sensitive compartmented information facilities (SCIFs). Typically, the procedures to meet these requirements are documented in approved site security plans.

Specific elements covered under this section are:

- Alarm annunciation and sensitivity
- Exterior and interior sensors
- Power supply
- Testing and maintenance
- Assessment and response
- Lighting.

To ensure compliance with DOE requirements, intrusion alarms and detection devices must perform within certain sensitivity specifications. Balanced magnetic switches (BMSs), volumetric detectors, and alarm connections to local law enforcement agencies (LLEAs) are also required to meet the applicable specifications.

In addition to patrols and visual surveillance provided by the protective force, alarm and detection devices are fundamental components of any PSS. To be effective, alarms must be clearly audible. Alarm displays must be clearly visible, must identify the location and type of alarm, and the operator interface must allow for alarm recognition by the operator. Alarm lines and other detection devices require continuous supervision to preclude any covert attempt to bypass the alarm system, and to ensure an appropriate and timely response. To achieve an acceptable degree of assurance that the PSS works properly, it is incumbent on facility management to provide for adequate equipment, an effective testing and maintenance program, and a sufficient number of trained personnel to operate the alarm and assessment equipment.

Intrusion-detection systems consist of both an alarm and an assessment system, and are usually layered for both interior and exterior applications. Exterior systems are designed to provide the earliest possible detection of an unauthorized intrusion, as far away from the security interests as possible. The interior intrusion-detection system may be even further divided into layers according to the configuration of security areas and the required levels of protection.

At SNM facilities, the outermost layer of the exterior systems is usually the perimeter intrusion-detection and assessment system (PIDAS). It typically consists of multiple and complementary electronic sensors, such as microwave, infrared, and electric field sensors; fence disturbance detectors; and seismic sensors. Exterior systems must be capable of withstanding the environmental conditions in which they are deployed. Properly designed systems generally use two or more types of complementary sensors, depending on the operating environment and design parameters. Typically, the PIDAS also includes fixed-position CCTV coverage for timely assessment of alarms generated in the PIDAS bed. PIDAS alarms normally annunciate in the CAS and SAS, where the alarm console operators can acknowledge the alarm, assess its cause, and direct a response as necessary.

Although design characteristics differ depending on the systems in use, the intent of the exterior sensor is to provide assurance that a person crossing the perimeter will be detected whether walking, running, jumping, crawling, rolling, or climbing at any point in the detection zone, under specified weight, and speed limits. Sensor systems are required to have adequate coverage in all weather and light conditions, overlap to eliminate dead areas, and be wide enough to deter bridging. Also, it is essential that detection zones contain no dips, high ground, or obstructions that could provide a pathway for an individual to avoid detection. CCTV systems used in conjunction with alarm and detection systems are most effective when they have the capability to automatically call the operator’s attention to an alarm-associated camera display, and the camera’s picture quality, field of view, and image size is such that the operator can easily recognize human presence. Tamper protection and loss-of-video alarm annunciation are essential characteristics of the system if the cameras serve as the primary means of alarm assessment. Video recorders, when used with the CCTV system and when initiated by alarm signals, are the most useful when they operate automatically and are rapid enough to accurately record an intrusion. Video capture systems, if used, provide pre-alarm, alarm, and post-alarm video images of the alarmed zone.

Interior intrusion-detection systems are normally designed to protect specific security areas (for example, PAs, LAs, MAAs, vaults, or vault-type rooms). These systems employ various technologies (for example, the detection of physical movement, heat, movement related to time, cable tension, vibration, pressure, and capacitance). Assessment means range from the deployment of protective forces to the use of multiple auto-focus camera systems equipped with pan/tilt and auto-zoom features.

Since alarms and detection systems require a power source for operation, it is necessary that an auxiliary power source consisting of batteries and/or generators be available, and that switchover is immediate and automatic if the primary power source fails. In most cases, immediate and automatic switchover will not occur if a generator is relied upon as the sole source of backup power; batteries are required to handle the immediate switchover, and the generator assumes the role once it obtains full power.

To ensure effective operation of alarms and detection devices, managers must provide for a regular test and maintenance program. Such a program includes the periodic testing of equipment and circuits, and the thorough inspection of equipment and circuits by qualified service personnel. Also, records on these tests are required to include the date of the test, name of the person conducting the test, and the results. Details on inspecting the testing and maintenance program are discussed in Section 7.

Frequently, intrusion-detection and entry-control systems are separate systems, interfaced to provide information to the system operator. In many systems, normal access control and other work-related activities are processed without operator interaction. Records of such transactions are generally recorded for historical purposes.

The main purpose of an intrusion-detection and assessment system is to alert the protective force to intrusion, aid in alarm assessment, allow the protective force to track intruder progress toward a target, and aid in assessing intruder activity and characteristics (for example, the number of intruders and whether they are armed). Protection systems normally include a suitable means to assess alarms and provide for an appropriate response; the protective force is usually responsible for monitoring and response. Also, protective force personnel are normally responsible for preparing alarm reports according to DOE or operations office specifications, and distributing copies as appropriate. Response procedures are usually found in the applicable site security plans.

Lighting is of primary importance in the operation of an effective alarm and detection system. Effective lighting provides a deterrent to adversary intrusion, assists the protective force in locating and assessing alarm initiations, and provides for effective use of CCTV as a surveillance and assessment tool. Lights are required to have a minimum specified luminescence at ground level for specific areas, a regular power source, and an emergency backup lighting capability. Lights should not cause glare or bright spots in CCTV camera images, especially if CCTV is the primary means of assessment.

Common Deficiencies/ Potential Concerns

False and Nuisance Alarms

One of the most common problems with intrusion-detection systems is that they may generate an inordinate number of false alarms. Many systems are susceptible to false and nuisance alarms induced by high winds, animals, heavy snow, lightning, vehicular vibration, and wind-blown dust and debris. These systems include microwave sensors, infrared sensors, electric field sensors, seismic sensors, and buried sensors. Improper installation (improper tension or insulation coupling) can also cause unacceptable false alarm rates on electric field sensors. Seismic sensors may produce nuisance alarms if installed too near fences, power poles, guy wires, or roads where vehicles generate heavy ground vibration. Video motion detectors are susceptible to nuisance alarms induced by reflected light, cloud motion, vehicle headlights, and camera vibration due to wind. A high rate of false and/or nuisance alarms may lead the protective force to ignore or improperly assess an unauthorized intrusion.

Improper Installation, Calibration, or Alignment

Improper installation, calibration, or alignment of sensors may significantly reduce sensitivity, contribute to false alarms, and allow for unauthorized intrusion. For example, insufficient offset may allow intruders to crawl under or jump over a bistatic microwave beam at the crossover point (the point where adjacent zones overlap). Also, video motion detectors require extensive maintenance and calibration for proper operation, and audio detectors must be calibrated carefully to avoid nuisance alarms caused by common background noises. Effective operation of a CCTV system is frequently diminished when the system is not correctly installed or aligned. If the camera is not properly placed or aligned, there may be “holes” in the coverage that permit an intruder to cross the isolation zone unobserved. Additionally, if the field of view of the camera is too long for the camera lens, an intruder at the extreme end of the field of view may not be adequately observed, or the camera’s automatic call-up feature may not operate quickly enough to capture adversary activity in the alarm zone.

Tamper Protection for Power Sources

The primary and backup power sources for intrusion-detection systems are susceptible to tampering. Power switches, inverters, and generators should be protected. These items are often overlooked during protection planning and installation. Exterior fuel tanks and filler points are especially vulnerable. For example, an inoperable filler point or contaminated fuel tank may nullify all backup power sources. If the primary power source fails, the protection systems become inoperable and DOE assets become vulnerable.

Inadequate Testing and Maintenance Program

Most PSS failures are the direct cause of an inadequate testing and maintenance program. Like an automobile, the lack of maintenance and operation (testing) usually results in equipment failure. For this reason, the testing and maintenance program is one of the most important features of any protection system. An effective program will normally include provisions that require facility technicians, augmented by service representatives, to perform all tests, maintenance, calibrations, and repairs necessary to keep the detection and assessment systems operational. An inadequate program that results in frequent system failure, cursory testing procedures, and an inordinate number of items of equipment awaiting repair are all indications of a lack of management attention. Details of inspecting the testing and maintenance program are discussed in Section 7.

Failure to Properly Assess and Respond

A number of factors may affect assessment and response. For example, a high rate of nuisance and false alarms may degrade operator response to genuine alarm conditions. Failure of a system to adequately identify alarm type and specific location may also degrade response. The latter is usually most evident when systems do not clearly differentiate between tamper-indication, line-supervision, and intrusion alarms, or when multiple sensors are monitored by a single circuit. For computer-based systems, problems may arise because of erroneous software modifications and system configurations that cause program errors. It is important that the signal received from the detection device provide identifiable evidence of the actual occurrence so operators can properly assess the situation and respond accordingly.

Planning Activities

During inspection planning activities, inspectors review available documents and interview points of contact. Elements to cover include:

- Review of the site mission (obtained from a review of the documents and from interviews with operations office personnel and site representatives)

- Review of organization charts; SSSP; site security plans and procedures; security plans for temporary MAAs; decontamination and decommissioning plans; waivers and exceptions, both approved and requested; past operations office survey reports and OA-10 inspection reports; site/facility asset list; site maps indicating location of layered security areas (LAs, PAs, MAAs, vaults, vault-type rooms), critical facilities, controlled areas, building definitions, locations of security posts, classified matter areas, vital equipment areas, SNM storage areas, and transfer routes

- Listing of the types of sensors employed; local alarm reporting devices; data-transmission systems; site lighting diagrams; console equipment descriptions; and alarm procedures

- Review of the assessment methodology employed (CCTV, video, and/or patrol response)

- Review of the vulnerability analysis (VA), including consideration of:

  – Application of the design basis threat

  – Review of site-specific threats to determine whether they address local characteristics, including the insider threat

  – Priority of site-specific threats

  – Target definition and locations

  – Graded and defense-in-depth PSSs

  – Pathways providing lowest detection and/or shortest delay

  – Presentation of the VA results in the SSSP

  – Listing of the protective elements identified in the VA for each security interest (review the VA results in the SSSP, along with site-specific VA methods and assessments not in the Master Safeguards and Security Agreement, to determine whether the key VA results are in the SSSP and whether any assumptions in the VA should be validated during the inspection)

- Comparison of vulnerabilities against findings and resolution of past OA-10 inspections and operations office surveys.

- Review of protective methods employed at the location to be inspected

- Type and location of potential targets (to further focus inspection efforts, compile a list of site assets, group them into appropriate categories, and determine potential impacts related to their loss).

Performance Tests

The following performance tests are recommended for alarms and intrusion-detection devices:

- Exterior perimeter sensors (Appendix A, Part 1)
- Interior sensors (Appendix A, Part 2)
- Perimeter CCTV (Appendix A, Part 3)
- Interior CCTV (Appendix A, Part 4)
- Alarm processing and display equipment (Appendix A, Part 5)
- Emergency auxiliary power supplies (Appendix D, Part 1)
- Tamper protection and line supervision (Appendix D, Part 2).

Data-Collection Activities

Alarm Annunciation and Sensitivity

A. Inspectors should review alarm records to determine false/nuisance alarm rates. This may involve reviewing alarm logs for a specified period (for example, two weeks) and determining the number of alarms during that period. Alternatively, the inspector could review the facility's plots of alarm rates if such plots are maintained. Any abnormally high alarm rates should be identified and the causes discussed with the facility representatives (including measures taken to eliminate false/nuisance alarm sources). The accuracy of alarm records can be investigated by comparing alarm plots against alarm logs or alarm plots/logs against computer records for a specified period. When reviewing alarm records, the inspector should clearly understand the facility's definitions of false alarms and nuisance alarms. This inspection should also consider interviewing alarm system operators to determine their understanding of false/nuisance alarm rates and make sure that they are consistent with facility definitions. The ability of operators to consistently make judgments as to whether alarms are considered false or nuisance will greatly affect false and nuisance alarm rate calculations.

Exterior and Interior Sensors

B. During inspection of the PIDAS, inspectors should examine the various types of sensors to determine whether they are complementary (that is, whether they consist of different sensor types that cannot be defeated by the same means, not just multiple layers of the same sensor). Inspectors should also confirm the existence of an effective testing and maintenance program for the PIDAS. Inspectors should check the condition of the PIDAS bed for obstructions, mounds and valleys, and other terrain features that an adversary could use to avoid the detectors. Crossover and interface points should also be checked to determine whether there are voids or blind spots in sensor coverage. Particular attention should be given to the identification of PIDAS sectors susceptible to bridging as a result of their close proximity to tall buildings, fences, telephone poles, or light and camera structures. Similar attention needs to be paid to any unsecured/unprotected accessway that tunnels beneath PIDAS sectors.

C. Inspectors should tour the CAS and SAS, visually inspect equipment, interview operators, and verify information gathered during document reviews. Items to be checked include operability of equipment, operators' familiarity with equipment, and measures to protect equipment from tampering. It is important that alarms reported from the field are properly recognized and acknowledged, and that appropriate responses are made. Interviews with station operators will reveal their understanding of their responsibilities.

D. At each exterior security area where a PIDAS is used, inspectors should determine the number and configuration of sensors, sensor alarm logic (for example, 1 of 2, 2 of 3), test frequency and methods, preventive maintenance frequency and methods, tamper-indicating provisions, and provisions for repairing component failures.

E. Inspectors should review documents and interview security staff to determine the method used to detect intrusion at each security area. If more than one method of detection is used at a security area (for example, an electronic alarm system and direct observation from guard towers), inspectors should determine how the systems complement each other; which is considered the primary means of detection; and whether the combination (primary and backup) is effective.

F. At selected interior security areas (for example, MAA buildings) and storage areas, inspectors should determine the types of sensors used to protect building perimeters (including doors, windows, and other penetrations), testing and preventive maintenance frequency and methods, tamper-indicating provisions, conditions for placing a zone portal in access, and provisions for repairing component failures.

G. Inspectors should determine whether the facility has more than one central electronic alarm system and, if so, the area that each system covers. A facility with two well-defined geographical areas may have a separate alarm system for each. For each separate electronic alarm system, inspectors should determine whether there are SASs, a central processing unit switching capability, tamper alarm features, and an adequate primary and backup power supply. This information can be gathered by document reviews or interviews with security staff. However, inspectors may need to interview the responsible system engineers to accurately determine the technical aspects of the system. Conducting such interviews in the CAS/SAS may allow a better understanding of the system and its interfaces.

H. Inspectors should verify that the SSSP identifies means for providing intrusion-detection capability when primary systems are out of service. Implementation of the measures can also be verified. This may involve reviewing the CAS or protective force supervisor logs or maintenance records to determine when equipment was out of service and to verify that compensatory measures were implemented during those periods.

Power Supplies

I. Backup or emergency auxiliary supplies are required for all security systems. Inspectors should validate the operability of these supplies. Testing of power supplies is normally conducted concurrently with the PIDAS lighting test and is referred to as the Emergency Generator Test (see Appendix D, Part 1).

Assessment and Response

J. Inspectors should verify complete coverage of the security area perimeter. This activity is particularly applicable at areas with alarmed fence lines that delineate a security area perimeter and that rely on protective force visual observation posts to assess alarms. An effective method of verifying complete coverage is to have one person walk the perimeter along the fence line while inspectors are stationed in the CAS observation posts assigned responsibility for that portion of the perimeter. Each portion of the perimeter can be checked sequentially. In this manner, the inspectors can verify that there are no blind spots along the perimeter that might permit an adversary to breach the boundary without being detected and assessed. This activity can be facilitated with two or more inspectors who “hopscotch” from post to post. The overlap points between zones can also be checked more readily with two or more inspectors in adjacent observation posts.

K. Inspectors should observe CCTV display monitors during a range of conditions, such as at different times of the day and night, and under various weather conditions if possible. Alternatively, the inspector may request facilities that have a video recording capability to provide tapes recorded during different weather conditions, if available. Inspectors should review the monitors or recordings to determine whether the CCTV systems provide appropriate data under varying light and weather conditions. Inspectors should also verify that camera and recorded video call-ups are rapid enough to capture adversary activity. This is usually done as part of the PIDAS inspection, once during the day and once at night, following the emergency auxiliary test for PIDAS lighting.

L. Inspectors should interview security staff and review documents to determine the areas where direct visual observation is the primary means of detecting intrusion or assessing alarms. Inspectors should determine the type of post (for example, tower, portal, continuous patrol), assessment aids available to protective force personnel (for example, search lights, night vision devices, binoculars), and the methods used by the facility to test effectiveness and maintain the SPO's level of vigilance. Inspectors should determine the operability of equipment, power supplies, measures to protect equipment from tampering, fields of view, adequacy of lighting, blind spots or obstructions, and overlap with adjacent zones.

Lighting

M. Inspectors should interview security staff, review documents, and conduct performance tests to determine lighting levels at portals, security area perimeters, exterior and interior areas that rely on CCTV, normal and emergency auxiliary supplies for lighting systems, procedures used if lighting fails, and methods for monitoring lighting systems and reporting and replacing burned-out lights and failed equipment.

N. Inspectors should observe the lighting during nighttime tours of the facility while lights are on primary power and then on auxiliary power. The lighting levels should be observed from a variety of locations, including key visual assessment posts (for example, towers). The CCTV monitors in the CAS/SAS and other selected posts (if any) should also be observed to determine the adequacy of lighting. One method of determining the adequacy of lighting is to have a person(s) (dressed in various contrastable color clothing) stand in various areas, as directed by the inspectors who are stationed in visual observation posts or monitoring CCTV cameras in the CAS/SAS. The inspectors should direct the individual to stand in locations where light levels are low or contrast ratios are high. The inspectors should determine whether there are blind spots and whether the lighting is adequate to distinguish between humans and animals at any location in the observation zone. If feasible, the lighting should be observed during a variety of conditions (for example, clear weather and rain or fog). Items to check include lighting levels, light/dark contrast, glare, shadows, and inoperative bulbs. Light meters may be used to check lighting levels and contrast ratios in various areas.

O. Inspectors should determine the vulnerability of lighting systems to sabotage by reviewing lighting circuit and power supply diagrams and touring areas critical to the lighting systems (for example, switchyards, transformers, circuit breakers, power lines, engine generators, uninterruptible power supply). Inspectors should determine whether all lights at a security area perimeter are on a single circuit (as opposed to having every other light on a second circuit), whether the electric power supplies are vulnerable to single point failures (for example, a circuit breaker), whether there are provisions for controlling access to areas containing components critical to the lighting system, self-testing features, methods for modifying system hardware and software, and whether there are provisions for maintaining assessment capability if the lighting fails.

This page is intentionally left blank.